ZILKA·KOTAB

PC

ZILKA, KOTAB & FEECE™

95 SOUTH MARKET ST. STE 420
SAN JOSE, CA 95113

TELEPHONE (408) 971-2573
FAX (408) 971-4660

FAX COVER SHEET

Date:	September 29, 2004	**Phone Number**	**Fax Number**
To:	Appeal Briefs- Patent		(703) 305-0942
From:	Kevin J. Zilka		

Docket Number: NAI1P157/00.091.01 **Application Number: 09/678,010**

Total Number of Pages Being Transmitted, Including Cover Sheet: 33

Please deliver to the Board of Patent Appeals & Interferences.

Thank you,

Kevin J. Zilka

☐ *Original to follow Via Regular Mail* X *Original will Not be Sent* ☐ *Original will follow Via Overnight Courier*

IF YOU DO NOT RECEIVE ALL PAGES OR IF YOU ENCOUNTER
ANY OTHER DIFFICULTY, PLEASE PHONE Erica
AT (408) 971-2573 AT YOUR EARLIEST CONVENIENCE

Practitioner's Docket No. NAI1P157/00.091.01 *PATENT*

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Lucas et al.

Application No.: 09/678,010 Group No.: 2131
Filed: 10/3/2000 Examiner: Chen, Shin Hon
For: PROVIDING BREAK POINTS IN VIRUS SCANNING OPERATION

Mail Stop Appeal Briefs – Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL OF APPEAL BRIEF

1. Transmitted herewith is the APPEAL BRIEF in this application, with respect to the Notice of Appeal filed on September 27, 2004.

2. STATUS OF APPLICANT

This application is on behalf of other than a small entity.

CERTIFICATION UNDER 37 C.F.R. §§ 1.8(a) and 1.10*

*(When using Express Mail, the Express Mail label number is **mandatory**; Express Mail certification is optional.)*

I hereby certify that, on the date shown below, this correspondence is being:

MAILING

_ deposited with the United States Postal Service in an envelope addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

37 C.F.R. § 1.8(a)
_ with sufficient postage as first class mail.

37 C.F.R. § 1.10*
_ as "Express Mail Post Office to Addressee"
Mailing Label No. _____ **(mandatory)**

TRANSMISSION

✓ facsimile transmitted to the Patent and Trademark Office, (703) 305-0942.

Date: 9/29/2004

Erica L. Farlow
Signature

Erica L. Farlow
(type or print name of person certifying)

** Only the date of filing (' 1.6) will be the date used in a patent term adjustment calculation, although the date on any certificate of mailing or transmission under ' 1.8 continues to be taken into account in determining timeliness. See ' 1.703(f). Consider "Express Mail Post Office to Addressee" (' 1.10) or facsimile transmission (' 1.6(d)) for the reply to be accorded the earliest possible filing date for patent term adjustment calculations.*

3. FEE FOR FILING APPEAL BRIEF

Pursuant to 37 C.F.R. § 1.17(c), the fee for filing the Appeal Brief is:

other than a small entity $330.00

Appeal Brief fee due $330.00

4. EXTENSION OF TERM

The proceedings herein are for a patent application and the provisions of 37 C.F.R. § 1.136 apply.

Applicant believes that no extension of term is required. However, this conditional petition is being made to provide for the possibility that applicant has inadvertently overlooked the need for a petition and fee for extension of time.

5. TOTAL FEE DUE

The total fee due is:

Appeal brief fee	$330.00
Extension fee (if any)	$0.00

TOTAL FEE DUE $330.00

6. PAYMENT OF FEES

The commissioner is authorized to charge deposit account 50-1351 (NAI1P157) in the amount of $330.00. A duplicate of this transmittal is attached.

7. FEE DEFICIENCY

If any additional extension and/or fee is required, and if any additional fee for claims is required, charge Deposit Account No. 50-1351 (Order No. NAI1P157).

Signature of Practitioner

Reg. No.: 41,429
Tel. No.: 408-971-2573
Customer No.: 28875

Kevin J. Zilka
Silicon Valley IP Group, PC
P.O. Box 721120
San Jose, CA 95172-1120
USA

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the application of	
Lucas et al.	Examiner: Chen, Shin Hon
Application No. 09/678,010	Art Unit: 2131
Filed: October 03, 2000	Date: September 29, 2004
For: PROVIDING BREAK POINTS IN VIRUS SCANNING OPERATION	

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

ATTENTION: Board of Patent Appeals and Interferences

APPELLANT'S BRIEF (37 C.F.R. § 41.37)

This brief is in furtherance of the Notice of Appeal, filed in this case on September 27, 2004.

The fees required under § 1.17, and any required petition for extension of time for filing this brief and fees therefor, are dealt with in the accompanying TRANSMITTAL OF APPEAL BRIEF.

This brief contains these items under the following headings, and in the order set forth below (37 C.F.R. § 41.37(c)(i)):

I REAL PARTY IN INTEREST
II RELATED APPEALS AND INTERFERENCES
III STATUS OF CLAIMS
IV STATUS OF AMENDMENTS
V SUMMARY OF CLAIMED SUBJECT MATTER

VI ISSUES

VII ARGUMENTS

VIII APPENDIX OF CLAIMS INVOLVED IN THE APPEAL

IX APPENDIX LISTING ANY EVIDENCE RELIED ON BY THE APPELLANT IN THE APPEAL

The final page of this brief bears the practitioner's signature.

I REAL PARTY IN INTEREST (37 C.F.R. § 41.37(c)(1)(i))

The real party in interest in this appeal is Networks Associates Technology, Inc.

II RELATED APPEALS AND INTERFERENCES (37 C.F.R. § 41.37(c)(1)(ii))

With respect to other prior or pending appeals, interferences, or related judicial proceedings that will directly affect, or be directly affected by, or have a bearing on the Board's decision in the pending appeal, there are no other such appeals, interferences, or related judicial proceedings.

Since no such proceedings exist, no Related Proceedings Appendix is appended hereto.

III STATUS OF CLAIMS (37 C.F.R. § 41.37(c) (1)(iii))

A. TOTAL NUMBER OF CLAIMS IN APPLICATION

Claims in the application are: 1-30.

B. STATUS OF ALL THE CLAIMS IN APPLICATION

1. Claims withdrawn from consideration but not canceled: None
2. Claims pending: 1-30
3. Claims allowed: None
4. Claims rejected: 1-30

See additional status information in the Appendix of Claims.

C. CLAIMS ON APPEAL

The claims on appeal are: 1-30

IV STATUS OF AMENDMENTS (37 C.F.R. § 41.37(c)(1)(iv))

As to the status of any amendment filed subsequent to final rejection, there are no such amendments after final.

V SUMMARY OF CLAIMED SUBJECT MATTER (37 C.F.R. § 41.37(c)(1)(v))

A method and computer program product are provided for detecting computer viruses within a computer file. As shown in Figure 3, for example, a request to scan a computer file for computer viruses is received. See operation 20. Next, a virus scanning operation is initiated upon the computer file. During the virus scanning operation, a measurement value is calculated. See operation 56 of Figure 4, for example. Such measurement value is indicative of an amount of data processing performed during the virus scanning operation. Further, the measurement value is based, at least in part, on at least one of a data size of the computer file and a complexity of tests of the virus scanning operation. Further during the virus scanning, the measurement value is compared with a threshold value. Note operation 58 of Figure 4, for example. If the measurement value exceeds the threshold value, a virus scanner break in the virus operation is then established, prior to completion of the tests to determine as to whether the computer file is infected. Note operation 60 of Figure 4, for example. See page 7, and page 8, lines 1-20, for example.

VI ISSUES (37 C.F.R. § 41.37(c)(1)(vi))

Following, under each issue listed, is a concise statement setting forth the corresponding ground of rejection.

Issue # 1: The Examiner has rejected Claims 1-3, 6-10, 11-13, 16-20, 21-23, and 26-30 under 35 U.S.C. 103(a) as being unpatentable over Nachenberg (U.S. Patent No. 5,826,031) in view of Banga et al. (U.S. Patent No. 6,240,447).

Issue # 2: The Examiner has rejected Claims 4, 5, 14, 15, 24, and 25 under 35 U.S.C. 103(a) as being unpatentable over Nachenberg (U.S. Patent No. 5,826,031) in view of Banga et al. (U.S. Patent No. 6,240,447) and further in view of Cozza (U.S. Patent No. 5,649,095).

VII ARGUMENTS (37 C.F.R. § 41.37(c)(1)(vii))

The claims of the groups noted below do not stand or fall together. In the present section, appellant explains why the claims of each group are believed to be separately patentable.

Issue #1:

The Examiner has rejected Claims 1-3, 6-10, 11-13, 16-20, 21-23, and 26-30 under 35 U.S.C. 103(a) as being unpatentable over Nachenberg (U.S. Patent No. 5,826,031) in view of Banga et al. (U.S. Patent No. 6,240,447).

Group #1: Claims 1, 11, and 21

The Examiner relies on the following excerpt from Nachenberg to make a prior art showing of appellant's claimed "calculating during said virus scanning operation a measurement value indicative of an amount of data processing performed during said virus scanning operation" (see all independent claims).

> "CDPE based methods employ additional heuristics to determine what the detection of various stoppers and boosters indicates about the code being emulated. For example, if a number of stoppers have been found prior to the detection of any boosters, the emulation control module will likely decide that the host file is uninfected. On the other hand, if one or more stoppers are detected following detection of a number of boosters, the emulation control module will likely decide that the polymorphic loop has been fully decrypted to reveal the static virus body. In this case, virus scanning will proceed." (col. 2, lines 15 - 25)

Appellant asserts that this excerpt in no way discloses, teaches, or even suggests "calculating during said virus scanning operation a measurement value indicative of an amount of data processing performed during said virus scanning operation." Nachenberg merely suggests the use of boosters, "sequences of instructions [that] are frequently found in polymorphic decryption loops", and stoppers, "sequences of

instructions [that] are rarely found in decryption loops" as a means for determining whether a file is infected.

In particular, the number of boosters and the number of stoppers are calculated during an emulation, and are compared against a threshold. As an example, Nachenberg states, "[i]f a number of stoppers have been found prior to a number of boosters, the emulation control module will likely decide that the host file is uninfected. On the other hand, if one or more stoppers are detected following detection of a number of boosters...virus scanning will proceed" (see Column 1, line 67 - Column 2, line 25).

This differs from appellant's claimed "calculating an amount of data processing performed during said scanning operation" in that Nachenberg is separately calculating a number of *identified and unidentified instruction sequences* as a means for determining whether a file is infected, while appellant claims calculating *an amount of data processed during the scan* to conditionally break virus scanning for preventing overload to the virus scanner, as claimed.

It is noted that, in the latest response mailed September 14, 2004, the Examiner further argued that the amount of boosters and stoppers constituted an amount of processing performed. Appellant respectfully disagrees with this assertion. Specifically, simply counting different types of instruction sequences (e.g. boosters and stoppers) for comparison purposes during emulation for the purpose of determining whether a file is infected in no way suggests appellant's claimed "calculating during said virus scanning operation a measurement value indicative of an amount of data processing performed during said virus scanning operation" to conditionally break virus scanning for preventing overload to the virus scanner (emphasis added).

Further in such latest response, it was argued by the Examiner that "Nachenberg does not explicitly disclose a measurement value indicative of an amount of data

processing performed, but Banga discloses a threshold value of data processed to increase the efficiency of the process." It thus appears that the Examiner has set forth conflicting assertions, namely that:

1. Col. 2, lines 15-25 of Nachenberg discloses appellant's claimed "calculating during said virus scanning operation a measurement value indicative of an amount of data processing performed during said virus scanning operation," and

2. "Nachenberg does not explicitly disclose a measurement value indicative of an amount of data processing performed."

Nevertheless, appellant has carefully reviewed Banga, and respectfully asserts that it still falls short of meeting appellant's claimed "calculating during said virus scanning operation a measurement value indicative of an amount of data processing performed during said virus scanning operation" (emphasis added). Only appellant teaches and claims such specific calculation at the time of virus scanning regarding an amount of data processing specifically in the context of a virus scanning operation.

The Examiner also cites the above excerpt as a prior art showing of appellant's claimed "wherein the measurement value is based, at least in part, on at least one of a data size of the computer file and a complexity of tests of the virus scanning operation" (see all independent claims). Contrary to the Examiner's assertion, appellant emphasizes that nowhere in Nachenberg, and especially nowhere in the above excerpt, is there even a suggestion of utilizing a test complexity value in determining whether a virus scanning should be terminated.

Appellant emphasizes that such a complexity value inherently represents the amount of data processing typically required to conduct a particular test, where such value may be used to conditionally trigger a break in virus scanning. The above excerpt

relied on by the Examiner simply discloses the use of boosters and stoppers as described above, and in no way even suggests appellant's claimed use of the "complexity of tests."

It is noted that, in the latest response mailed September 14, 2004, the Examiner now relies on the following excerpt from Nachenberg to make a prior art showing of appellant's claimed "wherein the measurement value is based, at least in part, on ... a complexity of tests of the virus scanning operation."

> "The selection of boosters and stoppers included in the emulation control module can have a substantial impact on the speed and accuracy with which the CDPE system detects viruses. Ideally, stoppers and boosters are selected to work accurately for all known polymorphic viruses. However, it may not be possible to find a set of such heuristics that does not significantly slow virus scanning. Stoppers and boosters useful for detecting several polymorphic viruses may actually prevent the detection of other polymorphic viruses, as for example, where a virus writer includes a standard stopper in polymorphic loop code to confuse CDPE modules. In general, any change in the stoppers or boosters used must be accompanied by extensive regression testing to insure that previously detected viruses are not missed using the new heuristics. Since new polymorphic viruses are continually being developed, the time consuming and awkward selection and regression testing of new combinations of stoppers and boosters can not be avoided." (col. 2, lines 26-40)
>
> "The speed of these programs is slowed further as more complicated heuristics are developed to detect polymorphic viruses.." (col. 6, lines 39-40)

In response, appellant notes that the foregoing excerpt merely suggests that heuristics are complicated. This in absolutely no way even suggests appellant's claimed calculation of a "measurement value that is based, at least in part, on ... a complexity of tests of the virus scanning operation." While Nachenberg may suggest that heuristics are complicated, it does not calculate, in the claimed manner, a measurement value based on such complexity.

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references

themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on appellant's disclosure. *In re Vaeck,* 947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

Appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all the claim limitations.

Group #2: Claims 2, 12, and 22.

With respect to the present group, the Examiner relies on the following excerpt from Nachenberg to make a prior art showing of appellant's claimed "step of, upon occurrence of said break, determining using said measurement value whether or not said virus scanning operation should be terminated prior to completion."

> "The dynamic exclusion module (240) examines the instruction/interrupt usage profiles (224) of each known polymorphic virus (150) as each instruction is fetched for emulation. The instruction/interrupt usage profiles (224) indicate which polymorphic viruses (150) employ mutation engines that do not use the fetched instruction in decryption loops they generate, and the emulation control module (220) flags these viruses. The emulation control module (220) continues until all mutation engines have been flagged or until a threshold number of instructions have been emulated. The flagging technique implemented by the dynamic exclusion module (240) determines when emulation has proceeded to a point where at least some code from the decrypted static virus body (160) may be scanned and substantially reduces the number of instructions emulated prior to scanning the remaining target files without resort to booster or stopper heuristics." (col. 3, lines 37-53)

While the foregoing excerpt may suggest "a break" (i.e. "continues until all mutation..."), such break is a break in emulation, not in virus scanning, as claimed

by appellant. Moreover, upon Nachenberg's "break," there is no "determining using said measurement value whether or not said virus scanning operation should be terminated prior to completion," as claimed.

Appellant again respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all the claim limitations.

Group #3: Claims 3, 13, and 23

With respect to such claims, the Examiner relies on the following excerpt from Banga to make a prior art showing of appellant's claimed "wherein said measurement value yields a processed data size value for data processed during said virus scanning operation."

> "According to this embodiment, the accumulated difference data are sent if T_{small} D and D_{tot} <F(S,C,T_{large}), where F is a function of the size of the original page, the size of the data that has been processed so far, and the threshold T_{large}. F generates a cut-off when it is no longer advantageous to send the difference data. The cut-off might be 80% of the original file size (0.8 S) based on cumulative bytes received. Alternatively, S could be ignored and the difference data would be sent as long as D_{tot} <0.8 C. More complicated functions can also be used." (col. 7, lines 1-10)

The foregoing excerpt appears to suggest a function, F, that is a function of a size of a page and a size of processed data. There is not, however, any suggestion of a "measurement value [that] yields a processed data size value for data processed during said virus scanning operation" (emphasis added).

Appellant again respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all the claim limitations.

Group #4: Claims 6, 16, and 26

With respect to Group #4, the Examiner again relies on the following excerpt from Banga to make a prior art showing of appellant's claimed "wherein said measurement value yields a processed data size value for data processed during said virus scanning operation and step of determining is responsive to both said processed data size value and a computer file size value for said computer file when determining whether or not said virus scanning operation should be terminated prior to completion."

> "According to this embodiment, the accumulated difference data are sent if T_{small} D and D_{tot} <F(S,C,T_{large}), where F is a function of the size of the original page, the size of the data that has been processed so far, and the threshold T_{large}. F generates a cut-off when it is no longer advantageous to send the difference data. The cut-off might be 80% of the original file size (0.8 S) based on cumulative bytes received. Alternatively, S could be ignored and the difference data would be sent as long as D_{tot} <0.8 C. More complicated functions can also be used." (col. 7, lines 1-10)

Again, the foregoing excerpt appears to suggest a function, F, that is a function of a size of a page and a size of processed data. There is not, however, any suggestion in the remaining Banga reference of a technique where the "step of determining is responsive to both said processed data size value and a computer file size value for said computer file when determining whether or not said virus scanning operation should be terminated prior to completion" (emphasis added). Only appellant teaches and claims conditionally terminating virus scanning after a break in such scanning, based on both a processed data size value and a computer file size value for the computer file.

Appellant again respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all the claim limitations.

Group #5: Claims 7, 17, and 27

With respect to the present group, the Examiner still yet relies on the following excerpt from Banga to make a prior art showing of appellant's claimed "wherein said step of determining calculates a measurement ratio of said processed data size value to said computer file size value and compares this with a termination size threshold ratio such that said virus scanning is terminated if said measurement ratio exceeds said termination size threshold ratio."

> "According to this embodiment, the accumulated difference data are sent if T_{small} D and D_{tot} <F(S,C,T_{large}), where F is a function of the size of the original page, the size of the data that has been processed so far, and the threshold T_{large}. F generates a cut-off when it is no longer advantageous to send the difference data. The cut-off might be 80% of the original file size (0.8 S) based on cumulative bytes received. Alternatively, S could be ignored and the difference data would be sent as long as D_{tot} <0.8 C. More complicated functions can also be used." (col. 7, lines 1-10)

Appellant again respectfully disagrees. There is not even a suggestion of a step that "calculates a measurement ratio of said processed data size value to said computer file size value and compares this with a termination size threshold ratio such that said virus scanning is terminated if said measurement ratio exceeds said termination size threshold ratio." Only appellant teaches and claims termination of virus scanning based on this specifically claimed calculation and comparison.

Yet again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all the claim limitations.

Group #6: Claims 8-9, 18-19, and 28-29

With respect to the present group, the Examiner relies on col. 1, line 63 – col. 2, line 50, and col. 6, lines 32-40 from Nachenberg to make a prior art showing of appellant's claimed "wherein said virus scanning operation applies a plurality of the tests to said computer file, each test having a complexity value indicative of an

amount of data processing associated with that test and said measurement value is a sum of complexity values for tests applied during said virus scanning operation."

After careful review of such cited excerpts, appellant respectfully asserts that simply nowhere in Nachenberg is there any sort of "virus scanning operation [that] applies a plurality of the tests to said computer file, each test having a complexity value indicative of an amount of data processing associated with that test and said measurement value is a sum of complexity values for tests applied during said virus scanning operation" (emphasis added). The cited excerpts from Nachenberg relate primarily to emulation, not virus scanning with the foregoing claimed testing features.

Appellant again respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all the claim limitations.

Group #7: Claims 10, 20, and 30

With respect to the present group, the Examiner cites col. 1, line 63 – col. 2, line 50, and col. 6, lines 32-40 from Nachenberg to make a prior art showing of appellant's claimed "virus scanning operation [that] applies a plurality of the tests to said computer file, each test having a complexity value indicative of an amount of data processing associated with that test, said measurement value being a sum of complexity values for tests applied during said virus scanning operation and said step of determining terminating said virus scanning operation prior to completion if said sum of complexity values exceeds a termination complexity threshold value."

However, simply nowhere in Nachenberg is there even a suggestion of determining a complexity value of a test, let alone summing up the complexity values of tests used to scan a file and comparing that sum to a threshold value for determining whether the scan should be terminated. The excerpts from Nachenberg cited by the

Examiner simply disclose boosters and stoppers as a means for determining whether a virus scan should proceed (see Column 1, line 63 - Column 2, line 50) and the use of virtual machines in emulating the polymorphic virus which creates slow operability (Column 6, lines 32-40). These excerpts do not even remotely suggest summing test complexity values to determine whether a virus scanning operation should be terminated, thus preventing overload of a virus scanner.

Appellant again respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all the claim limitations.

Issue # 2

The Examiner has rejected Claims 4, 5, 14, 15, 24, and 25 under 35 U.S.C. 103(a) as being unpatentable over Nachenberg (U.S. Patent No. 5,826,031) in view of Banga et al. (U.S. Patent No. 6,240,447) and further in view of Cozza (U.S. Patent No. 5,649,095).

Group #1: Claims 4, 5, 14, 15, 24, and 25

With respect to the present group, the Examiner cites Figure 4d and col. 6, lines 6-45 from Cozza to make a prior art showing of appellant's claimed "wherein said amount of data processing performed includes data processing involved in any decompression of said computer file required for said virus scanning operation."

In response, it is respectfully asserted that appellant is not merely claiming decompression, as suggested by Cozza, but rather calculates "a measurement value indicative of an amount of data processing performed during said virus scanning operation" ... "wherein said amount of data processing performed includes data processing involved in any decompression of said computer file required for said virus scanning operation." Only appellant teaches and claims conditionally

triggering a break in virus scanning based on such a specific measurement value (with respect to a threshold) that involves a decompression processing amount.

At least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all the claim limitations.

In view of the remarks set forth hereinabove, all of the independent claims are deemed allowable, along with any claims depending therefrom.

VIII APPENDIX OF CLAIMS (37 C.F.R. § 41.37(c)(1)(viii))

The text of the claims involved in the appeal (along with associated status information) is set forth below:

1. (Previously Amended) A method of detecting computer viruses within a computer file, said method composing the steps of:

receiving a request to scan a computer file for computer viruses;

initiating a virus scanning operation upon said computer file;

calculating during said virus scanning operation a measurement value indicative of an amount of data processing performed during said virus scanning operation, wherein the measurement value is based, at least in part, on at least one of a data size of the computer file and a complexity of tests of the virus scanning operation;

comparing during said virus scanning said measurement value with a threshold value; and

triggering a break in said virus operation prior to completion of the tests to determine as to whether the computer file is infected, if said measurement value exceeds said threshold value to prevent overload of a virus scanner.

2. (Original) A method as claimed in claim 1, further comprising the step of, upon occurrence of said break, determining using said measurement value whether or not said virus scanning operation should be terminated prior to completion.

3. (Original) A method as claimed in claim 1, wherein said measurement value yields a processed data size value for data processed during said virus scanning operation.

4. (Original) A method as claimed in claim 1, wherein said amount of data processing performed includes data processing involved in any decompression of

said computer file required for said virus scanning operation.

5. (Original) A method as claimed in claim 1, wherein said amount of data processing performed includes data processing involved in any unpacking of said computer file required for said virus scanning operation.

6. (Original) A method as claimed in claim 2, wherein said measurement value yields a processed data size value for data processed during said virus scanning operation and step of determining is responsive to both said processed data size value and a computer file size value for said computer file when determining whether or not said virus scanning operation should be terminated prior to completion.

7. (Original) A method as claimed in claim 6, wherein said step of determining calculates a measurement ratio of said processed data size value to said computer file size value and compares this with a termination size threshold ratio such that said virus scanning is terminated if said measurement ratio exceeds said termination size threshold ratio.

8. (Previously Amended) A method as claimed in claim 1, wherein said virus scanning operation applies a plurality of the tests to said computer file, each test having a complexity value indicative of an amount of data processing associated with that test and said measurement value is a sum of complexity values for tests applied during said virus scanning operation.

9. (Original) A method as claimed in claim 8, wherein said plurality of test applied are selected in dependence upon said computer file.

10. (Previously Amended) A method is claimed in claim 2, wherein said virus scanning operation applies a plurality of the tests to said computer file, each test having a complexity value indicative of an amount of data processing associated

with that test, said measurement value being a sum of complexity values for tests applied during said virus scanning operation and said step of determining terminating said virus scanning operation prior to completion if said sum of complexity values exceeds a termination complexity threshold value.

11. (Previously Amended) Apparatus for detecting computer viruses within a computer file, said apparatus comprising:

a receiver operable to receive a request to scan a computer file for computer viruses;

initiating logic operable to initiate a virus scanning operation upon said computer file;

calculating logic operable to calculate during said virus scanning operation a measurement value indicative of an amount of data processing performed during said virus scanning operation, wherein the measurement value is based, at least in part, on at least one of a data size of the computer file and a complexity of tests of the virus scanning operation;

comparing logic operable during said virus scanning to compare said measurement value with a threshold value; and

triggering logic operable to trigger a break in said virus operation prior to completion of the tests to determine as to whether the computer file is infected, if said measurement value exceeds said threshold value to prevent overload of a virus scanner.

12. (Original) Apparatus as claimed in claim 11, wherein, upon occurrence of said break, determining logic operates using said measurement value to determine whether or not said virus scanning operation should be terminated prior to completion.

13. (Original) Apparatus as claimed in claim 12, wherein said measurement value yields a processed data size value for data processed during said virus scanning operation.

14. (Original) Apparatus as claimed in claim 11, wherein said amount of data processing performed includes data processing involved in any decompression of said computer file required for said virus scanning operation.

15. (Original) Apparatus as claimed in claim 11, wherein said amount of data processing performed includes data processing involved in any unpacking of said computer file required for said virus scanning operation.

16. (Original) Apparatus as claimed in claim 12, wherein said measurement value yields a processed data size value for data processed during said virus scanning operation and said determining logic is responsive to both said processed data size value and a computer file size value for said computer file when determining whether or not said virus scanning operation should be terminated prior to completion.

17. (Original) Apparatus as claimed in claim 16, wherein said determining logic is operable to calculate a measurement ratio of said processed data size value to said computer file size value and compare this with a termination size threshold ratio such that said virus scanning is terminated if said measurement ratio exceeds said termination size threshold ratio.

18. (Previously Amended) Apparatus as claimed in claim 11, wherein said virus scanning operation applies a plurality of the tests to said computer file, each test having a complexity value indicative of an amount of data processing associated with that test and said measurement value is a sum of complexity values for tests applied during said virus scanning operation.

19. (Previously Amended) Apparatus as claimed in claim 18, wherein said plurality of tests applied are selected in dependence upon said computer file.

20. (Previously Amended) Apparatus as claimed in claim 12, wherein said virus scanning operation applies a plurality of the tests to said computer file, each test having a complexity value indicative of an amount of data processing associated with that test, said measurement value being a sum of complexity values for tests applied during said virus scanning operation and said step of determining terminating said virus scanning operation prior to completion if said sum of complexity values exceeds a termination complexity threshold value.

21. (Previously Amended) A computer program product carrying a computer program for controlling a computer to detect computer viruses within a computer file, said computer program comprising:

receiver code operable to receive a request to scan a computer file for computer viruses;

initiating code operable to initiate a virus scanning operation upon said computer file;

calculating code operable to calculate during said virus scanning operation a measurement value indicative of an amount of data processing performed during said virus scanning operation, wherein the measurement value is based, at least in part, on at least one of a data size of the computer file and a complexity of tests of the virus scanning operation;

comparing code operable during said virus scanning to compare said measurement value with a threshold value; and

triggering code operable to trigger a break in said virus operation prior to completion of the tests to determine as to whether the computer file is infected, if said measurement value exceeds said threshold value to prevent overload of a virus scanner.

22. (Original) A computer program product as claimed in claim 21, wherein, upon occurrence of said break, determining code operates using said measurement value to determine whether or not said virus scanning operation should be terminated prior to completion.

23. (Original) A computer program product as claimed in claim 22, wherein said measurement value yields a processed data size value for data processed during said virus scanning operation.

24. (Original) A computer program product as claimed in claim 21, wherein said amount of data processing performed includes data processing involved in any decompression of said computer file required for said virus scanning operation.

25. (Original) A computer program product as claimed in claim 21, wherein said amount of data processing performed includes data processing involved in any unpacking of said computer file required for said virus scanning operation.

26. (Original) A computer program product as claimed in claim 22, wherein said measurement value yields a processed data size value for data processed during said virus scanning operation and said determining code is responsive to both said processed data size value and a computer file size value for said computer file when determining whether or not said virus scanning operation should be terminated prior to completion.

27. (Original) A computer program product as claimed in claim 26, wherein said determining code is operable to calculate a measurement ratio of said processed data size value to said computer file size value and compare this with a termination size threshold ratio such that said virus scanning is terminated if said measurement ratio exceeds said termination size threshold ratio.

28. (Previously Amended) A computer program product as claimed in claim 21, wherein said virus scanning operation applies a plurality of the tests to said computer file, each test having a complexity value indicative of an amount of data processing associated with that test and said measurement value is a sum of complexity values for tests applied during said virus scanning operation.

29. (Previously Amended) A computer program product as claimed in claim 28, wherein said plurality of the tests applied are selected in dependence upon said computer file.

30. (Previously Amended) A computer program product as claimed in 22, wherein said virus scanning operation applies a plurality of the tests to said computer file, each test having a complexity value indicative of an amount of data processing associated with that test, said measurement value being a sum of complexity values for tests applied during said virus scanning operation and said step of determining terminating said virus scanning operation prior to completion if said sum of complexity values exceeds a termination complexity threshold value.

IX APPENDIX LISTING ANY EVIDENCE RELIED ON BY THE APPELLANT IN THE APPEAL (37 C.F.R. § 41.37(c)(1)(ix))

There is no such evidence.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 971-2573. For payment of any additional fees due in connection with the filing of this paper, the Commissioner is authorized to charge such fees to Deposit Account No. 50-1351 (Order No. NAI1P157_00.091.01).

Respectfully submitted,

By: _____ Date: 9/29/04

Kevin J. Zilka

Reg. No. 41,429

Zilka-Kotab, P.C.
P.O. Box 721120
San Jose, California 95172-1120
Telephone: (408) 971-2573
Facsimile: (408) 971-4660